

I. Amendments to the Claims

Please amend the claims as follows in accordance with revised 37 CFR § 1.121.

5 1. (Original) A method of enabling a proxy to participate  
in a secure communication between a client and a server,  
comprising the step of:

establishing a first secure session between the client  
and the proxy;

10 upon verifying the first secure session, establishing a  
second secure session between the client and the proxy, the  
second secure session requesting the proxy to act as a conduit  
to the server;

15 having the client and the server negotiate a session  
master secret; and

delivering the session master secret to the proxy using  
the first secure session to enable the proxy to participate in  
the secure communication.

20 2. (Original) The method as described in claim 1 further  
including the step of having the proxy use the session master  
secret and a session identifier to generate given  
cryptographic information.

3. (Previously presented) The method as described in claim 2 further including the step of having the proxy modify requests and responses following receipt of the session master secret and generation of the given cryptographic information.

4. (Previously presented) The method as described in claim 3 wherein the proxy performs a given service on behalf of the client while modifying content from the server.

5. (Original) The method as described in claim 4 wherein the given service is selected from a set of services including transcoding, caching, encryption, decryption, monitoring, filtering and pre-fetching.

6. (Original) The method as described in claim 1 wherein the first and second secure sessions confirm to a network security protocol.

7. (Original) The method as described in claim 6 wherein the network security protocol is SSL.

8. (Original) The method as described in claim 6 wherein the network security protocol is TLS.

9. (Original) The method as described in claim 1 wherein the server is a Web server and the client is a pervasive computing client.

10. (Original) A method of enabling a proxy to participate in a secure communication between a client and a server, comprising the step of:

5 having the client request a first secure connection to the proxy;

upon authenticating validity of a certificate received from the proxy, having the client request a second secure connection to proxy, the second secure connection requesting the proxy to act as a conduit to the server;

10 having the proxy generate a session identifier;

having the client and the server negotiate a session master secret through the conduit;

15 upon completion of the negotiation, having the client deliver the session master secret to the proxy using the first secure connection;

having the proxy use the session master secret and the session identifier to generate given cryptographic information that is useful for participating in the secure communication.

20 11. (Previously presented) The method as described in claim 10 further including the step of having the proxy modify requests and responses following receipt of the session master secret and generation of the given cryptographic information.

12. (Previously presented) The method as described in claim 11 wherein the proxy performs a given service on behalf of the client while modifying content from the server.

5 13. (Original) The method as described in claim 12 wherein the given service is selected from a set of services including transcoding, caching, encryption, decryption, monitoring, filtering and pre-fetching.

10 14. (Original) The method as described in claim 10 wherein the first and second secure sessions confirm to a network security protocol.

15 15. (Original) The method as described in claim 14 wherein the network security protocol is SSL.

16. (Original) The method as described in claim 14 wherein the network security protocol is TLS.

17. (Original) A method for establishing the security of a session between a client and a server, comprising the steps of:

through a proxy, conducting a security handshake procedure between the client and the server to produce a session key; and

transmitting the session key to the proxy so that the proxy can participate in communications between the client and the server during the session.

18. (Original) The method as described in claim 17 wherein the session key is transmitted from the client to the proxy over a secure connection.

19. (Original) The method as described in claim 18 wherein the secure connection between the client and the proxy is created before the security handshake procedure and is maintained throughout the session.

20. (Currently Amended) A cryptographic system,  
comprising:

a client;

a server;

a proxy;

a network protocol service for enabling the client and  
server to communicate over a secure connection;

a computer program product in a computer readable medium

(i) for controlling the client to request a first secure  
connection to the proxy, (ii) responsive to authenticating  
validity of a certificate from the proxy, for controlling the  
client to request a second secure connection to proxy, the  
second secure connection requesting the proxy to act as a  
conduit to the server, (iii) for controlling the client to  
negotiate with the server through the conduit to obtain a  
session master secret; and (iv) upon successful completion of  
the negotiation, for controlling the client to deliver the  
session master secret to the proxy using the first secure  
connection; and

a computer program product in a computer readable medium

(i) for controlling the proxy to use the session master secret  
and a session identifier to generate given cryptographic  
information, and (ii) for having the proxy modify content in  
communications between the client and the server.

21. (Original) The cryptographic system as described in claim 20 wherein the proxy includes means for providing transcoding services on behalf of the client.

5

22. (Original) The cryptographic system as described in claim 20 wherein the proxy includes means for providing encryption/decryption services on behalf of the client.

10 23. (Original) The cryptographic system as described in claim 20 wherein the proxy includes means for providing caching services on behalf of the client.

15 24. (Original) The cryptographic system as described in claim 20 wherein the proxy includes means for providing monitoring services on behalf of the client.



25. (Previously presented) A computer program product in a computer readable medium for use in a cryptographic system including a client, a server, and a proxy, comprising:

5 a first routine (i) for controlling the client to request a first secure connection to the proxy, (ii) responsive to authenticating validity of a certificate from the proxy, for controlling the client to request a second secure connection to proxy, the second secure connection requesting the proxy to act as a conduit to the server, (iii) for controlling the  
10 client to negotiate with the server through the conduit to obtain a session master; and (iv) upon successful completion of the negotiation, for controlling the client to deliver the session master secret to the proxy using the first secure connection; and

15 a second routine (i) for controlling the proxy to use the session master secret and a session identifier to generate given cryptographic information, and (ii) for having the proxy modify content in communications between the client and the server.